What is claimed is:

1. A machine-implemented method comprising:

examining a set of instructions embodying an invoked application to identify the invoked application;

obtaining an application-specific intrusion detection signature; and

monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion.

2. The method of claim 1, further comprising tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

3. The method of claim 2, wherein tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds.

4. The method of claim 3, wherein at least one of the one or more configurable thresholds comprises a threshold set by monitoring communications for the invoked application during a defined time window.

5. The method of claim 2, wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

6. The method of claim 5, wherein the network intrusion detection system component and the invoked application run within a single execution context.

7. The method of claim 6, further comprising:

providing a first application-specific remedy for a detected intrusion; and

providing a second application-specific remedy for identified application-specific abnormal communication behavior.

8. The method of claim 7, wherein providing a first application-specific remedy comprises cutting at least a portion of the network communications for the invoked application, and wherein providing a second application-specific remedy comprises notifying a system administrator of the identified application-specific abnormal communication behavior.

9. The method of claim 6, wherein obtaining the

application-specific intrusion detection signature comprises loading the application-specific intrusion detection signature from a local signature repository.

10. The method of claim 6, wherein obtaining the application-specific intrusion detection signature comprises:

requesting the application-specific intrusion detection signature from a local signature repository in communication with a remote signature repository; and

receiving the application-specific intrusion detection signature from the local signature repository.

11. The method of claim 6, wherein the set of instructions reside in a file, and wherein examining the set of instructions comprises:

applying a hash function to data in the file to generate a condensed representation of the data; and

comparing the condensed representation with existing condensed representations for known applications.

12. A machine-readable medium embodying machine instructions for causing one or more machines to perform operations comprising:

examining a set of instructions embodying an invoked

application to identify the invoked application;

obtaining an application-specific intrusion detection signature; and

monitoring network communications for the invoked application using the application-specific intrusion detection signature to detect an intrusion.

13. The machine-readable medium of claim 12, wherein the operations further comprise tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

14. The machine-readable medium of claim 13, wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

15. The machine-readable medium of claim 14, wherein the network intrusion detection system component and the invoked application run within a single execution context.

16. The machine-readable medium of claim 15, wherein the operations further comprise:

providing a first application-specific remedy for a detected intrusion; and

providing a second application-specific remedy for identified abnormal communication behavior.

17. The machine-readable medium of claim 16, wherein the first and second application-specific remedies each comprise cutting at least a portion of the network communications for the invoked application.

18. The machine-readable medium of claim 15, wherein obtaining the application-specific intrusion detection signature comprises:

requesting the application-specific intrusion detection signature from a signature repository; and

receiving the application-specific intrusion detection signature from the signature repository.

19. The machine-readable medium of claim 18, wherein the signature repository comprises a local signature repository in communication with a remote signature repository.

20. The machine-readable medium of claim 15, wherein examining the set of instructions comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

21. A system comprising:

a network;

a security operation center coupled with the network; and

one or more machines coupled with the network, each machine comprising a communication interface and a memory including an execution area configured to perform operations comprising examining a set of instructions embodying an invoked application to identify the invoked application, obtaining application-specific intrusion criteria, and monitoring network communications for the invoked application using the application-specific intrusion criteria to detect an intrusion.

22. The system of claim 21, wherein the application-specific intrusion criteria comprises a normal communication behavior threshold.

23. The system of claim 21, wherein the application-specific intrusion criteria comprises an intrusion signature.

24. The system of claim 21, wherein monitoring network communications comprises monitoring network communications in a network intrusion detection system component running in an execution context with the invoked application.

25. The system of claim 24, wherein the operations further comprise providing an application-specific remedy for a detected intrusion.

26. The system of claim 25, wherein providing an application-specific remedy comprises cutting at least a portion of the network communications for the invoked application.

27. The system of claim 24, wherein each machine further comprises a local repository, the security operation center includes a master repository, and wherein obtaining the application-specific intrusion criteria comprises:

requesting the application-specific intrusion criteria from the local repository;

requesting the application-specific intrusion criteria from the master repository if the application-specific intrusion criteria is unavailable in the local repository;

receiving the application-specific intrusion criteria from the master repository if requested; and

receiving the application-specific intrusion criteria from the local repository.

28. The system of claim 24, wherein examining the set of instructions comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

29. A system comprising:

a security operation center;

one or more machines, each machine including means for identifying a process, obtaining a process-specific intrusion detection signature, and monitoring network communications for the process using the process-specific intrusion detection signature to detect an intrusion; and

communication means coupling the one or more machines with the security operation center.

30. The system of claim 29, wherein each machine further includes means for tracking one or more characteristics of the network communications to identify process-specific abnormal communication behavior.